



RECOMMENDATIONS *for* TRANSFORMING CLASSIFICATION

[RECOMMENDATION 1]: *The President should appoint a White House-led Security Classification Reform Steering Committee to oversee implementation of the Board's recommendations to modernize the current system of classification and declassification.* This committee would exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the transformation of the security classification system. The Senior Information Sharing and Safeguarding Steering Committee provides a good model for the committee. Its chair should be appointed and granted specific authorities by the President.⁸ Members of the committee should be knowledgeable and experienced senior officials from the national security community, as well as officials responsible for federal information technology, records management, and public information policy and practice. It should have the authority to enact the changes recommended by the Board: identifying and implementing new initiatives, policies, and standards in support of transformation. The committee would establish, monitor, and enforce priorities and corresponding benchmarks and timeframes for meeting specific goals, reporting successes and shortcomings to the President. The Board recognizes that to be successful, the implementation process itself must be transparent and earn support from both Government agencies and the public. The Board will be available to assist the committee in carrying out the President's direction by monitoring and evaluating agency implementation efforts.

[RECOMMENDATION 2]: *Classification should be simplified and rationalized by placing national security information in only two classification categories, aligned to existing practices in much of the government.* Top Secret will remain and retain its current, high level of protection. All other classified information would be categorized at a Lower-Level (to be named), which would follow standards for a lower level of protection. Both categories would include compartmented and special access information, as they do today. The two categories should be defined and distinguished by the level of

identifiable protection needed to safeguard and share information appropriately; these identifiable levels of protection would determine whether classification is warranted and at what level. The new model will require all classified information to continue to be subject to declassification and all other requirements of Executive Order 13526.

The Board's study revealed the concern by users about the increasing complexity of the classification system and accelerating growth of classified records, and confirmed a practical need to simplify policies and practices and make the system more usable. We believe that the system, in practice, need not be complex. The goal of reforming the system is to align classification levels with actual safeguarding practices throughout government. This alignment, when used in combination with accurate classification guidance linking clearly identifiable risk to classification level, will result in more precise and appropriate classification. Accurate classification most certainly aids future declassification activity, and we believe two-levels of classification may lead to less classification overall. There is a need to define more precisely and narrowly what types of information warrant security classification. The two-tiered system of classification will prod agencies to reexamine the current broad definitions of information that qualifies for classification.

The actions consequent to classifying align to only two levels of protection in Government-wide safeguarding disciplines: two levels of security clearance investigations, two levels of physical safeguarding and two levels of information systems domains. There is a practical need to simplify current policies and practices to make the system more usable. The Board found that classifying agencies in the U.S. Government and our international partners share this concern. In the case of international partners, some are moving to a two-tiered model similar to that recommended by the Board.⁹ In the case of U.S. agencies, some already are operating in a de-facto two-tiered model, though the levels of classification vary (i.e.

| New Classification Category | Old Classification Category | Level of Protection | |
|------------------------------|-----------------------------|----------------------------|---|
| Higher-Level "Top Secret" | Top Secret | Higher level of protection | Includes compartmented and special access information |
| Lower-Level | Confidential and Secret | Lower level of protection | |

some classify almost exclusively at the CONFIDENTIAL/SECRET levels, while for others SECRET/TOP SECRET predominate).

[RECOMMENDATION 3]: *The decision to classify information and at what level in the two-tiered system should be more clearly defined and distinguished by the level of identifiable protection needed to safeguard and share information appropriately.* The threshold for classifying in the two-tiered system should be adjusted to align the level of protection with the level of harm anticipated in the event of unauthorized release. This can only be achieved by *linking clearly identifiable risk* to an accurate harm assessment in classification guidance. Classifiers then would only be required to identify *the corresponding minimum level of protection* needed to ensure appropriate safeguarding and facilitate required information sharing. Determining a level of protection to facilitate or limit dissemination is more prescriptive in practice and would assist classifiers in making more accurate classification decisions. Applying this risk management practice by identifying the level of protection needed based on the sensitivity of the information, rather than potential damage if disclosed, would allow users to classify information

at the lowest level of protection or to keep the information unclassified.

Classification guidance would need to be revised to reflect the two-tiered model, with the goals of reducing over-classification, improving authorized information sharing, and not focusing solely on the dangers of inappropriate disclosure. Guidance would clearly define levels of protection by identifying a specific consequence of release of the classified information and the potential harm to the national security of limiting the sharing of the information. The difficulty of applying the current concept of presumed “damage” during derivative classification would be replaced by a more concrete application of the level of protection necessary for sharing and protecting. This change in guidance would reflect how classification is actually practiced by derivative classifiers—deciding how much protection is needed based on the sensitivity of the information to both protect and share appropriately.

The best way to deal with over-classification and promote information sharing is to manage risk by correctly assessing potential harm and classifying to meet the minimum

CLASSIFICATION GUIDANCE UNDER THE RECOMMENDED SYSTEM WOULD ADDRESS

the specific consequences and potential harm to the national security of unauthorized release and of limitations on the sharing the information. This guidance will also provide classifiers more information at the time of classification about any likelihood the information would need to be shared with state, local, or tribal governments during a crisis. A risk management protocol would aid in deciding whether the potential harm of inadvertent release would entail more damage than the inability to share the information on a broader level and would direct classification accordingly. Currently, classification decisions are based on the loosely defined levels of presumed “damage” found in Executive Order 13526. These decisions are often made without regard to the public or tactical value of disclosure and reflect an institutional risk-averse culture that results in systematic over-classification.

★ ★

“The best way to ensure that secrecy is respected, and that the most important secrets remain secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall.”

*Report of the Commission on Protecting and Reducing Government Secrecy,
1997, Senate Document 105-2, Public Law 236.*

level of protection needed, or often even keeping the information unclassified. When considering classifying, every classifier should give serious consideration to declassification and strive to better balance the need to protect information with the public’s right to access information about its government.

Confidential and Secret information in the current system require similar levels of protection against unauthorized release.¹⁰ Classifiers are often unable to distinguish between the criteria for applying the Confidential and the Secret markings and default to the higher classification, erring on the side of protection. More difficult still is judging when to apply the criteria for the Confidential marking rather than refraining from any classification. In the simplified model, tighter definitions keyed to identifiable risks and sharper description of the protections under the new Lower-Level

category should help classifiers make better decisions. The new two-tiered classification model should not simply combine the Confidential and Secret categories of classification. Although some information previously marked as Confidential may receive the Lower-Level marking in the new model, much more information should remain unclassified in the first instance. In order to simplify the system and classify less, agencies will need tighter definitions, better measures of identifiable risk and level of protection, clearer standards for access to information, and robust, new training to implement these changes.

The creation of a new Lower-Level classification category will ease the burden placed on users needing to share information that is not of the highest sensitivity. Access controls in this Lower-Level category will be the most instrumental factor in protecting information. The new

THE SIMPLIFICATION OF THE CLASSIFICATION SYSTEM TO A TWO-TIERED MODEL IS not without meaningful challenges for agencies, particularly the Departments of State and Energy. In the FY 2011 Annual Report to the President, agencies reported to ISOO the use of Confidential in 15.2% of their total classification decisions; the State Department’s use was at 27% and 61% of its original classification decisions were at the Confidential level.¹¹ Diplomatic conversations are regularly classified as Confidential. In its meetings with senior agency officials at the State Department, the Board learned that the State Department (and many other agencies) already operates in a de facto two-tiered classification system. Currently, the State Department classifies primarily at the Confidential and Secret levels. In the new, two-tiered model the information will continue to be classified where an identifiable risk mandates a level of protection, but at the Lower-Level.

The Department of Energy must navigate between two regimes of classification: for Classified National Security Information (under Executive Order 13526) and for nuclear information, known as Restricted Data information (under the Atomic Energy Act).¹² Some Restricted Data information currently bears a Confidential marking, though its level of protection is roughly equivalent to that of Secret national security information. It will require substantial effort to harmonize and clarify the markings and protections within these two regime

PRESENTLY, THE INTELLIGENCE AND DEFENSE COMMUNITIES STRIVE FOR GREATER information sharing on their electronic networks¹³ through a two-tier classification level strategy:

| <i>Network</i> | <i>Category</i> | <i>Level of Protection for Classified Information</i> |
|----------------|-----------------|---|
| JWICS | Top Secret/SCI | Higher level of protection compared to Secret |
| SIPRNET | Secret | Lower level of protection compared to Top Secret |
| NIPRNET | Unclassified | N/A* |

*The NIPR network contains appropriate protection levels afforded controlled, unclassified information (CUI).

Lower-Level category will enable information technology platforms to support and share classified information consistently across user domains. More unified security policy should facilitate greater system integration and improved protection. Compartmented and special access information, including Sensitive Compartmented Information, would be held, as appropriate, in either the Top Secret or the new Lower-Level category, with access tightly controlled.

[RECOMMENDATION 4]: *The specific protections afforded intelligence sources and methods need to be precisely defined and distinguished.* Intelligence sources and methods require special evaluation when determining classification. The ability to safeguard and share this type of information appropriately depends on the capacity to distinguish between intelligence and non-intelligence sources. Intelligence methods, in particular, must be more precisely defined in classification guidance to aid appropriate classification and, ultimately, declassification. The Board recognizes the compelling need to mitigate risk within this specific information grouping because of its high sensitivity.


[RECOMMENDATION 5]: *Pre-decisional, tactical, and operational information with short-lived sensitivity*

should be identified and segmented for automatic declassification without further review. This type of time-specific classified information should be declassified automatically without any review *only after* the pertinent specific event occurs or date passes. It should be classified and marked as “Short-term” (or similar term) at creation, and technology should be employed to automate the declassification action. Agency declassifiers may offer expertise on the type of information that could be marked in this category. The automatic declassification of “Short-term” information would save valuable resources and inform the historical record of decisions and actions at the earliest time, hopefully earning public support and improving agency relationships with partners.

[RECOMMENDATION 6]: *Agencies should recognize in policy and practice a “safe harbor” protection for classifiers who adhere to rigorous risk management practices and determine in good faith to classify information at a lower level or not at all.* Classifiers face incentives that bias their decisions toward classification. They should be encouraged and rewarded—and at least not punished—for good-faith decisions that certain information should remain unclassified. Some agencies currently exercise these provisions and should be recognized

“Put positively, a new classification system should maintain classification for the shortest possible time and make the declassification system more efficient rather than more costly.”

Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994, Joint Security Commission



IN OPERATION DESERT STORM, THE UNITED STATES LED A UNITED NATIONS-authorized coalition force from 34 nations in a war against Iraq after its invasion and annexation of Kuwait. The initial action to expel Iraqi troops from Kuwait began with an aerial bombardment on January 17, 1991, followed by a ground assault on February 23. Coalition forces liberated Kuwait decisively, halted its advance into Iraqi territory, and declared a cease-fire after only 100 hours of the ground campaign.

Command of this large-scale conflict was conducted in a mostly digital environment through the use of leadership video conferencing, battlefield reporting and other digital media coordination. Much of the operational and tactical military information regarding Operation Desert Storm, including records “born-digital,” could have been classified and marked as “Short-term” at the time the records were created. The cease-fire declared on February 28, 1991, could have been the occasion for automatically declassifying some specific, time-limited information no longer requiring protection, including born-digital information. Such automatic declassification of born-digital information would lessen the burden of preserving this information from format obsolescence and enable study by the government and civilian historical communities at the earliest permissible time.

and serve as models of “best practice” for establishing procedures and training programs that encourage classification challenges. In addition to new policies, implementing this recommendation will depend on a fundamental change in culture and longstanding practice. Classification training should address the deep-rooted cultural bias that favors classification, and often over-classification, through coordinated, consistent education that underscores the responsibility to not classify if in doubt.

Changing the culture of classification also will require effective training in the proper use of the classification system. The Information Security Oversight Office historically has found that the quality of classification training programs varies significantly across agencies, and that many of these programs are deficient. The President should direct the Security Classification Reform Steering Committee to examine agencies’ training programs and

develop a strong model for training that draws on best practices.

From discussions with Executive branch officials, the Congress, and the public, the Board recognizes that over-classification impedes access to information for all users, including the public. It also undermines the integrity of the system. Agencies should be required to conduct separate training units on over-classification, which could include illustrative examples, case studies of resulting harms, an explication of the limits of the authority of derivative classifiers, and other pertinent information. This would ensure meaningful adherence to Executive Order 13526’s requirement that classifiers be trained in avoiding over-classification. The Board recommends using incentives to encourage challenges to classification that would increase oversight and help shift the culture bias from favoring classification to one that recognizes the opportunity found in and need for declassification.¹⁴